

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Records and information stored at premises controlled by META
PLATFORMS, INC. ("the Provider"), headquartered in Menlo Park,
California pertaining to FACEBOOK ACCOUNT USER ID:
100005729952718

Case No.

22-m-698

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Records and information stored at premises controlled by META PLATFORMS, INC. ("the Provider"), headquartered in Menlo Park, California pertaining to FACEBOOK ACCOUNT USER ID: 10000572995271; see attachment A located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

2250(a)

Failure to Register as a Sex Offender

The application is based on these facts:

See attached affidavit.

☐ Continued on the attached sheet.

☒ Delayed notice of _____ days (give exact ending date if more than 30 days: 12/28/2022) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Rodney Clauss, Deputy U.S. Marshal

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date:

7/26/2022

Judge's signature

City and state: Green Bay, Wisconsin

James R. Sickel, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK ACCOUNT **USER ID:**
100005729952718 THAT IS STORED AT
PREMISES CONTROLLED BY META
PLATFORMS, INC.

Case No. _____

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Rodney Clauss, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I am a Deputy United States Marshal with the United States Marshals Service and, as such, am charged with enforcing all laws in all jurisdictions of the United States, its territories, and possessions. I have been a member of the United States Marshals Service for twenty-two (22) years and have investigated multiple fugitive cases. I have had both formal training and participated in numerous investigations to locate federal and state fugitives. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. §

2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2250(a) have been committed by Jeffrey J. Cox ("Jeffrey"). There is also probable cause to search the information described in Attachment A for evidence of these crimes [[and contraband or fruits of these crimes]], as described in Attachment B.

PROBABLE CAUSE

5. The United States government, including the USMS, is investigating violations of Title 18, United States Code, Section 2250(a) committed by Jeffrey.

6. On October 6, 2008, Jeffrey was convicted in Brown County Circuit Court, case number 08CF403, of 2nd Degree Sexual Assault of a Child. Based on that conviction, Jeffrey is required to register as a sex offender in Wisconsin for life.

7. On July 15, 2019, the Wisconsin Department of Corrections (WI DOC), issued a warrant for Jeffrey for a Parole Violation. Jeffrey was under supervision of the WI DOC for the underlying sex conviction, Brown County case number 08CF403.

8. On October 2, 2019, an additional warrant was issued by the Brown County Sheriff's Department for Jeffrey for a Sex Offender Registration Violation in Brown County case number 19CF1496.

9. On August 27, 2020, Jeffrey was charged in Brown County with two additional charges; Felon in Possession of a Firearm and Injury by Negligent Handling of a Dangerous Weapon. According to information obtained from the Brown County criminal complaint, Jeffrey was a passenger in a vehicle when a witness observed Jeffrey “messing around with a handgun he took from a backpack.” The witness stated, Jeffrey was “racking the slide and taking the magazine out and putting it back in. All of a sudden the gun went off and the sound was very loud.” The driver of the vehicle began to scream as she was shot in the back by Jeffrey.

10. To this date, the Green Bay Police Department has made multiple attempts to locate Jeffrey in the Green Bay area by conducting surveillance at last known addresses and interviewing known associates of Jeffrey. Green Bay PD Detective Biller provided me with an active Facebook account for Jeffrey. That Facebook account name is “Vincentia Son”. The User ID for that account is 100005729952718.

11. Upon review of Facebook account “Vincentia Son”, I discovered that it is an active Facebook account with fourteen public messages posted in the month of June (2022). On June 6, 2022, Jeffrey posted a picture of himself with an unknown male. I compared that Facebook photograph I believed to be Jeffrey and determined he matched a Brown County Jail booking photograph known to be Jeffrey. I noted that additional photographs posted to that same Facebook account also matched several Brown County Jail booking photographs of Jeffrey.

12. I discovered additional information located on Facebook account “Vincentia Son”. Under “Intro”, the user posted “From Chicago, Illinois” and “Lives in Chicago, Illinois.” Based on my training and experience, Facebook “users” often enter this information when creating and updating a Facebook account.

13. Based on my training and experience in locating and apprehending fugitives, the data being sought by this warrant will assist in locating Jeffrey. Because successful apprehensions often rely on the element of surprise, it is often necessary to attempt an arrest during nighttime or the early morning hours, when most people are sleeping. Further, apprehension tactical plans often change at the last minute based on unexpected movements or other behavior of the target. Therefore, I cannot predict in advance when this data would need to be accessed and would need access to the data at all times of the day or night in order to ensure a safe and successful apprehension.

14. As of the date of this affidavit, Jeffrey's whereabouts remain unknown, and all three arrest warrants mentioned above remain unserved. In addition, an open SORNA investigation will remain open until Jeffrey is located and apprehended.

15. Meta owns and operates Facebook, a free-access social networking website that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

16. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

17. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual

Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

18. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

19. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

20. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can “tag” other users in a photo or video and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

21. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats of the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

22. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

23. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

24. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

25. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

26. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

27. In addition to the applications described above, Meta provides users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about the user’s access or use of that application may appear on the user’s profile page.

28. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user’s IP address is retained by Meta along with a timestamp.

29. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables “Location History,” “checks-in” to an event, or tags a post with a location.

30. Social networking providers like Meta typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

31. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

32. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the foregoing, I request that the Court issue the proposed search warrant.

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

36. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Rodney Clauss
Deputy US Marshal
US Marshals Service

Subscribed and sworn to before me on July 26, 2022



James Sickel
United States Magistrate Judge



ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook account **User ID:**
100005729952718 that is stored at premises owned, maintained, controlled, or operated by Meta
Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, for **User ID: 100005729952718**, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.]]
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities **August 10, 2020 to the present**;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them **August 10, 2020 to the present**, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification

numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user **August 10, 2020 to the present**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests;
- (g) All “check ins” and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (j) All information about the Facebook pages that the account is or was a “fan” of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the account **August 10, 2020 to the present**;
- (m) All information about the user’s access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 14 DAYS of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 2250(a), involving Jeffrey since **August 10, 2020**, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (b) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (c) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. ("Meta"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. such records were generated by Meta's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature